Investigating the User Experience of Smartphone Authentication Schemes - The Role of the Mobile Context

Matthias Baldauf
Institute for Information and Process Management
University of Applied Sciences St.Gallen
St.Gallen, Switzerland
matthias.baldauf@fhsg.ch

Sebastian Steiner
INSO Research Group
TU Wien
Vienna, Austria
sebastian.steiner@inso.tuwien.ac.at

Mohamed Khamis
Glasgow Interactive Systems Section
School of Computing Science
University of Glasgow
Glasgow, UK
mohamed.khamis@glasgow.ac.uk

Sarah-Kristin Thiel
Department of Computer Science
Aarhus University
Aarhus, Denmark
thiel@cs.au.dk

Abstract

Today's smartphones feature several authentication methods not only to protect the overall device but also to control access to mobile banking and commerce apps, for example. However, to date there is no clear understanding on how users perceive different authentication methods in light of different usage contexts. To close this gap, we report on a study (N=22) in which we compared four recent authentication schemes on Android devices (Face Unlock, fingerprint scanning, NFC ring and PIN) in four different mobile settings (private vs. public, moving vs. stationary). We found that Fingerprint scanning turned out to be a well-suited and accepted authentication scheme over all four investigated contexts. While the NFC-based ring authentication is seen as less suitable for private settings, Face Unlock is disliked for public settings.

1. Introduction

As the most ubiquitous and personal devices in history, smartphones contain and give access to a myriad of private and sensitive information. They store vast amounts of photos, contain e-mails, chat messages and calendar entries, comprise long histories of visited Web pages and let users interact with their social network. Furthermore, installed sports and health trackers unveil the owner's physical condition, banking apps reveal her financial status and respective m-commerce and payment apps even enable costly online and offline purchases.

Figure 1. We compared four authentication schemes for smartphones with regard to four mobile contexts: face unlock, fingerprint scanning (left), NFC ring unlock (right) and PIN (exemplary illustrations).

To prevent unwanted access, either in case we shortly leave our phones unattended or, worse, the phone is stolen, today's smartphones offer a variety of authentication schemes. These include traditional ones such as entering a secret code, biometrics-based schemes such as fingerprint scanning, as well as token-based ones which check for the close vicinity of a smart personal item. These methods can not only be used to control access to the phone in general (i.e., its operating system) but are also increasingly applied to protect privacy-critical applications such as mail, banking or payment apps (either configurable by the user or forced by the provider). On average, users unlock their phones 50 times a day [1].

While prior work in the field of usable and secure smartphone authentication suggests that one single authentication scheme might not be practical across different mobile contexts [2], research about

URI: https://hdl.handle.net/10125/59918
ISBN: 978-0-9981331-2-6

how users perceive the use of particular currently available authentication methods in different mobile usage contexts is scarce. Yet, this practical knowledge is valuable for interaction designers and developers of both mobile apps and operating systems. For example, researchers and practitioners can benefit from recommendations on which authentication schemes are suitable according to the type of app, or how to customize a scheme according to the context.

To close this gap, we conducted a lab study with 22 participants. We compared four widely available authentication schemes [3, 4] on Android devices: PINs, fingerprint scanning (Figure 1, left), face unlock, and NFC ring (Figure 1, right) and investigated their setup procedures as well as their perceived comfort of use and suitability in four different mobile settings (private vs. public, moving vs. stationary). We discuss the implications of the study results and provide suggestions for practitioners and researchers.

2. Background and Related Work

We build on (1) smartphone authentication, (2) usability and security trade-off, and (3) context-dependent authentication.

2.1. Smartphone Authentication

Motivated by the need for privacy protection on mobile devices [5], research in Mobile HCI brought forth a variety of authentication schemes. They can be generally classified to 1) *Knowledge-based schemes* [6, 7, 8, 9, 10], where the user has to *know* something (e.g., PIN or pattern) to unlock, 2) *Possesion-based schemes* [11, 12], where the user has to *posses* a token (e.g., NFC ring, or personal mobile device), 3) *Inherence-based schemes* or biometric schemes [13, 14], which rely on biometric data such as fingerprint, eyes behavior, face detection etc. In our work, we investigate how the context influences the users' perception of these different authentication factors.

2.2. Usability and Security Trade-off

It is widely accepted that security is usually a secondary rather than a primary goal for users when performing daily tasks [15]. Harbach et al. found that users do not perceive shoulder surfing as a risk [1]. Eiband et al. explained this when they found that shoulder surfing does occur in the real world, but often goes unnoticed [16]. Eiband et al. also found that authentication credential (e.g., PINs and patterns) are among the data often shoulder surfed, and that there could be serious consequences to shoulder surfing that affect not only data security but even personal safety. This highlights the importance of using secure authentication schemes to protect users from shoulder surfing, and prevent its negative consequences. Many of today's most commonly used authentication schemes are vulnerable to shoulder surfing [16], thermal attacks [17], and smudge attacks [18].

However, systems that are more secure yet less usable are less likely to be used in practice. Harbach et al. reported on the results of an online survey and a field study in which they investigated users' smartphone unlocking behavior [1]. They found that users spend 2.9% of their interaction times authenticating, and unlock their phones 47.8 times a day on average [1]. This underlines the need for *fast* authentication schemes, since every additional second spent authenticating accumulates to large amount of time. De Luca et al. [19] conducted an online survey on the reasons for using and not using biometric authentication systems on smartphones and conclude that usability is a more relevant decision factor than privacy or trust issues. Harbach et al. [1] found that there are many contexts in which users do not perceive the need for secure authentication (e.g., at home), which motivates the need for context-dependent authentication [20].

2.3. Context-dependent Authentication

Several solutions from research and industry exploit knowledge about the user's context to enhance the user authentication experience. Prior works proposed using the location of the user to decide which security measures to take [21, 20, 22]. For example, many systems (e.g., banking apps and *Facebook*) ask additional questions when logging in using an unusual IP, and *Google's Smart Lock*[1] does not lock the screen when the user is at home. Due to the trade-off between usability and security, these schemes often offer more security at the expense of lower usability. For example, multiple authentication systems, such as *GazeTouchPIN* [23] and *SwiPIN* [9], were proposed with the intention to be used *only* when resistance to shoulder surfing is needed, since they are slightly slower than their less secure counterparts. *SnappApp* uses PIN for secure access, and a sliding gesture for fast access; the fast access mode restricts the apps that can be launched and has a time limit [24]. Furthermore, there are apps on the *Google Play* store that assign different lock mechanisms for each mobile application [25, 26].

We build over prior work by contributing practical insights into the perception of widely available mobile authentication schemes in typical mobile contexts.

[1] https://get.google.com/smartlock/

3. Method

In this section, we describe our study method and present details on the participants, the investigated authentication schemes, and the study setup and design.

3.1. Participants

The call for participation in the study was distributed by the authors via social media and emails to direct personal contacts with the request to further distribute the call. As a precondition, potential participants had to own their smartphone for at least half a year and use it multiple times a day. We applied a nonprobabilistic sampling, yet carefully selected interested ones with varying working (students, young and experienced professionals) and educational (apprentices, students, graduates, practitioners) backgrounds. Out of the finally chosen 24 participants, we had to exclude two for the actual study due to problems with the fingerprint scanner: Both were chemistry students and stated that they often had issues with fingerprint scanners due to minor corrosive injuries at their fingers from acidic substances. 13 of the final participants were female, nine male. The subjects were aged between 20 and 54 years (M=27.05, MD=25.00). 17 participants owned a smartphone for over three years, three for two to three years and two participants one to two years. Six of the participants used smartphones with iOS and 16 with Android. Five of the 22 participants did not have German as their native language but considered their German language skills sufficient for the study. They were offered to set the phone to their native language but refused.

3.2. Authentication Schemes

For comparison, we selected four authentication schemes due to their wide availability and, in case of the NFC ring, due to their novelty. Note that we used Android devices, i.e. the following descriptions refer to the respective Android implementations.

Android Face Unlock (in the remainder simply referred to as *Face Unlock*) uses facial image recognition. For authentication, a photo of the current user's face taken by the front camera is compared to one or several photos locally stored during setup. This feature has been available on Android smartphones since Android 5.0 (published in 2014). At its publication time, Face Unlock was the first widely available face recognition software that could be used on smartphones for authentication purposes. Although it can be bypassed with a photo of the smartphone owner, it is still available on current Android smartphones. However, during setup the user is informed about this security risk.

Fingerprint scanning has been introduced for mobiles by the Toshiba G500 and G700 in 2007. However, the authentication scheme gained popularity mostly because of *Touch ID*, *Apple*'s brand and implementation of fingerprint authentication introduced with the *iPhone 5s* in 2013. Sporadic Android devices featured fingerprint scanners before, yet fingerprint recognition became part of the standard platform (and thus could be used by third-party apps) with Android 6.0 in 2015. Similar to Face Unlock, during an authentication attempt the scanned data is compared with a locally stored version of the fingerprint.

The **NFC ring**, worn on a finger, is an example for a recent token-based authentication scheme relying on a smart personal item. *Near Field Communication* (NFC) is a wireless short-range communication technology. Respective rings contain so-called NFC tags which can be detected by the NFC sensors integrated on the backside of most modern smartphones. Thus, for authentication the ring needs to be placed in front of the sensor. Again, the identifier of the scanned tag is compared with the one configured during setup. In contrast to similar authentication methods using Bluetooth technology (to detect a trusted smartwatch, for example) with a range of dozens of meters, NFC-based authentication only works within a few centimeters. Respective rings and a corresponding authentication app are available from *McLear* [2] since 2016, for example.

PIN (Personal Identification Number), a multi-digit passcode, is a traditional knowledge-based authentication method. It is typically used at ATMs for debit and credit cards or for physical access control. On mobile phones PINs have been available since the early beginnings, to protect SIM card access, for example. To unlock the smartphone the user has to enter a number, usually consisting of at least four digits. Again, for a successful authentication the entered PIN must match the previously defined one.

3.3. Setup

The study was conducted in two separate adjacent test rooms. We prepared two recent mass-market smartphones from Sony, a *Sony Xperia X* and a *Sony Xperia Z3 Compact*. Both were running *Android* in version 7.

For the NFC Ring Unlock method we provided the model "Signature" by *McLear Ltd.* and installed the corresponding mobile application in version 1.7.3. This application was also the reason for using two

[2] https://nfcring.com/

smartphones: it does not replace the original Android unlock screen but adds another authentication layer that becomes visible only after the user has successfully unlocked the phone. To be able to correctly compare the investigated authentication methods in terms of speed and usage comfort, the ring unlock was used on a separate phone without any additional "on-board" authentication.

On the other smartphone, the test assistant who conducted the study, switched between the fingerprint scanner, the PIN and the Face Unlock during the study.

3.4. Study Design

We invited the participants in groups of four to six persons (five test sessions overall). The groups deliberately consisted of persons who did not know each other. Each of the test sessions started with a briefing on the topic and the study outline by the test assistant and a short questionnaire gathering demographic data and prior experience (knowledge and usage of the investigated authentication methods, for example).

Then, each test person, one by one, was asked to initially set up the authentication methods in a separate room. The order of the four methods was systematically varied following a Latin square to avoid any learning or preference effects. For each method, the present test assistant clocked the time it took the participants to successfully set up the scheme. After the final method, the participants were asked to rank the four methods in terms of setup complexity, i.e. to assign the numbers 1 (worst) to 4 (best) to the four schemes.

In the second test phase, the test assistant asked the participants to explore the four authentication schemes and unlock the phones several times in four different contexts (again, orders were systematically varied):

- **Moving - Private**: Each participant explored the methods in a separate room while walking.
- **Moving - Public**: Each participant explored the methods in the room with the other participants while walking.
- **Stationary - Private**: Each participant explored the methods in a separate room while sitting.
- **Stationary - Public**: Each participant explored the methods in the room with the other participants while sitting next to them.

In all study settings, the test assistant was present and made notes about observations and comments of the respective participant. Having tested each authentication method in one context, the participants were asked to rank them in terms of the comfort of use in the specific context. Having completed all contexts, the participants ranked the methods with regard to the perceived suitability of each method for a public, private, moving and stationary setting.

4. Results

In the following, we present the quantitative and qualitative results of our study. To test for significant differences ($p<.05$), we ran ANOVA tests. For post-hoc pairwise comparisons we used Bonferroni corrected confidence intervals. Error bars in the figures indicate the standard error.

Concerning prior knowledge and experience, 21 participants knew the PIN method, 19 had used it at least once. 18 participants knew fingerprint scanning, 6 had used it themselves on their smartphone. Face Unlock and NFC-based unlocking were known by three participants, respectively. Yet, none of the participants had used one of those two methods before.

4.1. Setup Duration and Complexity

Figure 2 (left) shows the average duration for setting up the four authentication methods. Our participants were fastest with the PIN method (M=45.18s, SD=15.08s), followed by the fingerprint scanner (M=66.55s, SD=23.45s) and the Face Unlock (M=69.59s, SD=18.71s). Setting up the NFC ring unlock took the most time (M=76.45s, SD=16.40s). The post-hoc pairwise tests show that the setup of the PIN method is significantly faster that the studied alternatives ($p<.001$).

This outcome correlates with the perceived setup complexity (Figure 2, right): the setup of the PIN method was rated simpler than the alternatives (M=3.77, SD=.61). The setup of the fingerprint scanner was ranked second-simplest (M=2.32, SD=.84) followed by the one of the Face Unlock (M=2.10, SD=.92). The setup of the NFC ring unlock method was rated as most complex (M=1.82, SD=.96). Again, the result of the PIN method differs significantly from the three other authentication schemes ($p<.001$).

4.2. Comfort of Use

Figure 3 shows the results of the participants' rankings regarding the comfort of use grouped by the investigated mobile contexts. The fingerprint scanner received the highest ratings (M between 3.23 and 3.45) in each context. Pairwise post-hoc tests reveal that its use is perceived as significantly more comfortable than the Face Unlock and the NFC ring unlock in all mobile

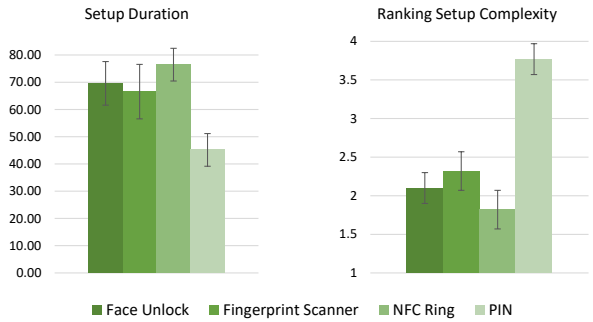

Figure 2. A comparison of the initial setup of the four authentication methods: the average setup duration in seconds (left) and the perceived setup complexity (1-worst to 4-best) (right).

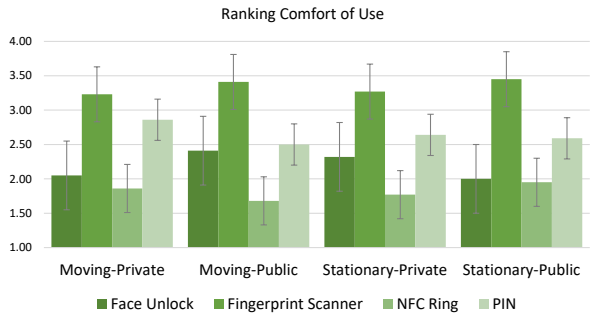

Figure 3. Ranking of the perceived comfort of the four authentication methods in four mobile contexts.

contexts ($p<.01$).

The PIN method was ranked second-best in all contexts in terms of the comfort of use (M between 2.50 and 2.86), was rated significantly better ($p<.03$) than the NFC ring unlock in each context but 'Stationary - Public'. Lowest scores regarding comfort of use received Face Unlock (M between 2.00 and 2.41) and NFC ring unlock (M between 1.68 and 1.95).

Comparing the comfort of use over different contexts, we observe the same order of authentication methods.

4.3. Suitability for Contexts

Figure 4 shows the summary of how our participants ranked the suitability of the four authentication methods for the mobile contexts *public*, *private*, *moving* and *stationary*.

For public settings, the participants ranked the fingerprint scanner (M=3.72, SD=.63) significantly better than the alternatives ($p<.001$). The NFC ring and PIN were rated second with similar results. Face Unlock was rated significantly worse than the other authentication schemes ($p<.02$) for this scenario.

For private settings there is no clear favorite: Face Unlock, fingerprint scanning and PIN received similar ratings with non-significant differences. Yet, the NFC unlock ring (M=1.59, SD=.73) was ranked significantly worse than the other methods ($p<.003$).

When moving, the participants again ranked the fingerprint scanner (M=3.68, SD=.71) significantly better than the rest ($p<.001$) and the PIN method (M=2.64, SD=.79) significantly better than Face Unlock and the NFC ring ($p<.03$).

For the "stationary" scenario, our participants rated the suitability of fingerprint scanning (M=3.14, SD=.99) significantly better than the suitability of the NFC ring ($p<.001$). Also Face Unlock (M=2.5, SD=1.26) and PIN (M=2.72, SD=.94) were perceived significantly more suitable than the NFC ring for this scenario ($p<.03$).

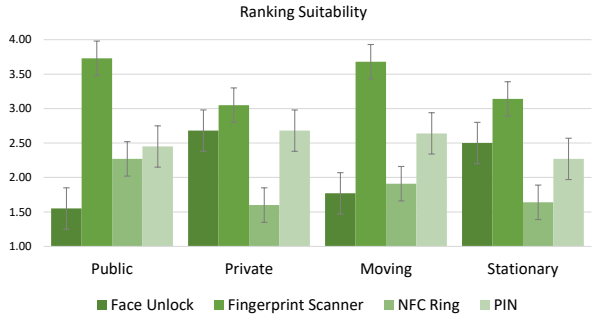

Figure 4. The perceived suitability of the four authentication methods for four mobile contexts: public, private, moving and stationary.

4.4. Observations and Participants' Comments

In this section, we summarize qualitative findings from observations during the study as well as verbal comments from participants.

Face Unlock caused the most problems during setup. Only six out of the 22 participants were able to find the corresponding option in the settings menu without any help from the test assistant. A majority of the participants stated that this feature and its setup was unnecessarily hidden and circuitous. Moreover, participants complained about the minimalistic user feedback during unlock. A successful face scan is only communicated by a small icon transforming into an open lock. A "swipe to unlock" gesture is still required to leave the lock screen.

Eleven participants had negative remarks regarding the actual face scanning ("it feels like I'm taking selfies", "holding up the phone is exhausting", "this is unpleasant to use in public").

Nine participants mentioned the performance (speed and recognition rate) of Android's Face Unlock in a positive light and considered it as a "fancy" technology.

Setting up **fingerprint scanning** was difficult for seven participants. The prompts used in the setup screens turned out to be ambiguous, leaving many participants puzzled about how to correctly move the finger over the sensor.

The majority of the participants had very positive remarks for its use ("very quick and simple", "ideal to unlock the smartphone in an unnoticeable way", "you always have your finger with you"). Often the smartphone was unlocked so quickly that the participants did not notice that it already happened and asked whether they unintentionally removed all the previously set up unlock methods.

NFC Ring Unlock was perceived very differently by participants. Positive statements included that the NFC Ring Unlock method is something new and thus interesting. On the opposite, many of the participants claimed that they do not like rings in general or that the used ring was not stylish enough.

Two participants stated that the ring requires direct contact to the NFC sensor (instead of one or two centimeters range) and that this fact makes a lot of difference for the usability of the technology. One tech-savvy participant additionally commented that support from the operating system would be better than the currently used additional application for detecting the ring.

Most participants mentioned that they liked the idea, however, that it takes time to accustom oneself to the correct usage. Furthermore, they noticed that such an item could be lost or forgotten easily or shift its position on the finger.

PIN entry caused no noticeable problems for the participants during setup. Although it was not specified, all the participants chose a four-digit PIN. Most of the participants stated that they are used to it and that they use PINs frequently in various contexts. Two participants stated that they prefer other methods over PIN because they are afraid of shoulder surfing attacks. A few participants commented that this authentication method required the most interaction with the smartphone.

5. Discussion

In our study, the traditional PIN outperformed the three more recent alternatives in both setup duration and perceived setup complexity. We ascribe this to the facts, that the PIN method is very well-known, the setup process is straight-forward and does not involve any ambiguous steps as well as the vast majority is familiar with entering PINs. With regard to the setup, the three other investigated authentication schemes performed similarly poor. In most cases, the reasons were usability issues (corresponding option cannot be found, ambiguous prompts, etc.). We conclude from this findings, that app developers should rather avoid forcing users to use a previously not configured modern authentication scheme such as fingerprint scanning, Face Unlock or NFC-based authentication. Problems during setup might affect a user's overall experience of the third-party app.

Regarding the comfort of use, it turned out that the users' perception of the respective authentication schemes is very similar in different contexts, i.e. the mobile context does not significantly impact the perceived comfort of use. The investigated authentication schemes seem technically mature, the comfort of Face Unlock was not negatively affected in the moving scenarios, for example. Our participants favored fingerprint scanning: Once configured, current fingerprint scanning worked very fast and highly robust. We ascribe the low rankings of Face Unlock and the NFC ring to the insufficient user feedback and the unnatural hand and finger placement to correctly position the ring in front of the NFC sensor, respectively.

Concerning the suitability for different contexts, Face Unlock was perceived as least suitable in public settings. From the participants' remarks we learned that they felt exposed and thought to arouse attention due to the camera-based detection. This result of our "hands-on" study confirms findings from the online survey by De Luca et al. [19], who report on awkwardness when using Face Unlock in public. We therefore do not recommend Android Face Unlock for protecting apps typically used in public such as payment apps in a queue at the checkout.

Fingerprint had a high suitability score in each context and therefore, can be recommended for apps typically used in all of the four investigated scenarios. According to our participants it works fast and (due to the fingerprint reader mounted at backside of the phone) can be easily integrated into the typical handling of the phone when taking it out of a bag, for example. Remarkable are the high scores in public settings and moving context, which qualifies it especially for payment apps or running and fitness tracker apps.

NFC ring had rather low suitability scores in all contexts and received its best rating for public settings. As reason, we assume that after some training during the setup phase, the users were able to authenticate with the ring rather unobtrusively (in contrast to Face Unlock, for example) what is an appreciated attribute of smartphone

authentication schemes. However, we conclude that NFC-based authentication using a small external token which can be easily lost or forgotten, is not appreciated for mobile contexts at all.

The suitability of the PIN method was perceived as similarly good in all investigated scenarios, yet always received lower scores than fingerprint scanning. We therefore recommend it as a general well-accepted authentication scheme and, in case an application already applies fingerprint scanning, as a suitable back-up solution.

6. Limitations

In the present study, we focused on the users' perception of the studied authentication methods. We deliberately ignored any security aspects, either subjective or objective, and performance aspects such as error rates of the discussed methods.

We tried our best to mimic the "public setting" in a controllable environment by having multiple unknown persons present during the test of a participant. However, we assume, yet cannot guarantee that this situation conveyed a truly realistic impression of a public setting such as in a busy shop, for example.

Again, we emphasize that the study participants used Android devices. Therefore, the results do not demand for cross-platform generalization. This is especially important for the biometrics-based authentication schemes. For example, on Apple devices the fingerprint sensors are integrated into the front (in contrast to the study devices with fingerprint sensors at the back side). Moreover, Apple's facial recognition system *Face ID* is based on infrared technology and thus might perform and thus be experienced differently in respective comparative studies.

7. Conclusion and Outlook

We presented a comparative lab study investigating users' perceived comfort of use and suitability of four recent smartphone authentication methods in four different mobile contexts. Our results indicate that the four investigated contexts do not affect the experienced comfort of use of the investigated method. Yet, we learned that users assess the methods' suitability differently across various contexts. Face Unlock is disliked for public settings, while the NFC-based ring authentication is seen as less suitable for private settings. Fingerprint scanning turned out to be a well-suited and accepted authentication scheme over all four investigated contexts.

Furthermore, we found that setting up the biometric authentication schemes in Android is difficult for many users. Usability flaws include insufficient user feedback, ambiguous prompts and hard to find menu items. Third-party app developers should consider these obstacles when suggesting a respective authentication scheme or even forcing users to initially configure fingerprint scanning or Face Unlock.

Follow-up studies should try to validate the presented findings in the field (e.g., using the participants' personal devices and mobile questionnaires, e.g.) to proof the ecological validity of our results. Additionally, such a field study should investigate long-term effects (e.g., how the perceived usability of a recent authentication scheme such as the NFC ring) changes over time.

Prospective in-depth studies could further explore potential factors (such as the form factor and appearance of a token-based mobile authentication scheme) impacting the comfort of use and the perceived suitability. For example, a nice-looking ring might be preferred over less pretty one in public settings. Furthermore, future studies could focus on the users' authentication experiences of app categories with different security or privacy requirements.

Finally, future studies should consider further methods and platforms. Especially, the most recent mobile authentication scheme available on mass market phones, Apple's *Face ID* should be compared to former face unlock implementations. An advanced implementation with a more tolerant recognition might make this authentication method less noticeable and more suitable for public settings.

8. Acknowledgments

The authors would like to thank the volunteers who participated in the presented study.

References

[1] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, (Menlo Park, CA), pp. 213–230, USENIX Association, 2014.

[2] A. De Luca and J. Lindqvist, "Is secure and usable smartphone authentication asking too much?," *Computer*, vol. 48, no. 5, pp. 64–68, 2015.

[3] M. Harbach, A. De Luca, and S. Egelman, "The anatomy of smartphone unlocking: A field study of android lock screens," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, (New York, NY, USA), pp. 4806–4817, ACM, 2016.

[4] E. von Zezschwitz, P. Dunphy, and A. De Luca, "Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices,"

in *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '13, (New York, NY, USA), pp. 261–270, ACM, 2013.

[5] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, and S. Möller, "On the need for different security methods on mobile phones," in *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, MobileHCI '11, (New York, NY, USA), pp. 465–473, ACM, 2011.

[6] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, "Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, (New York, NY, USA), pp. 2937–2946, ACM, 2014.

[7] J. Gugenheimer, A. De Luca, H. Hess, S. Karg, D. Wolf, and E. Rukzio, "Colorsnakes: Using colored decoys to secure authentication in sensitive contexts," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '15, (New York, NY, USA), pp. 274–283, ACM, 2015.

[8] M. Khamis, F. Alt, M. Hassib, E. von Zezschwitz, R. Hasholzner, and A. Bulling, "Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices," in *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '16, (New York, NY, USA), pp. 2156–2164, ACM, 2016.

[9] E. von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "Swipin: Fast and secure pin-entry on smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, (New York, NY, USA), pp. 1403–1406, ACM, 2015.

[10] Y. Yang, G. D. Clark, J. Lindqvist, and A. Oulasvirta, "Free-form gesture authentication in the wild," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, (New York, NY, USA), pp. 3722–3735, ACM, 2016.

[11] M. Khamis, R. Hasholzner, A. Bulling, and F. Alt, "Gtmopass: Two-factor authentication on public displays using gaze-touch passwords and personal mobile devices," in *Proceedings of the 6th ACM International Symposium on Pervasive Displays*, PerDis '17, (New York, NY, USA), pp. 8:1–8:9, ACM, 2017.

[12] F. Schaub, P. Lang, B. Könings, and M. Weber, "Prical: Dynamic privacy adaptation of collaborative calendar displays," in *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*, UbiComp '13 Adjunct, (New York, NY, USA), pp. 223–226, ACM, 2013.

[13] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: Implicit authentication based on touch screen patterns," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, (New York, NY, USA), pp. 987–996, ACM, 2012.

[14] C. Song, A. Wang, K. Ren, and W. Xu, ""eyeveri: A secure and usable approach for smartphone user authentication"," in *IEEE International Conference on Computer Communication (INFOCOM'16)*, (San Francisco, California), pp. 1 – 9, April 2016.

[15] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security," *BT Technology Journal*, vol. 19, pp. 122–131, Jul 2001.

[16] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt, "Understanding shoulder surfing in the wild: Stories from users and observers," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, (New York, NY, USA), pp. 4254–4265, ACM, 2017.

[17] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt, "Stay cool! understanding thermal attacks on mobile-based user authentication," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, (New York, NY, USA), pp. 3751–3763, ACM, 2017.

[18] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proceedings of the 4th USENIX Conference on Offensive Technologies*, WOOT'10, (Berkeley, CA, USA), pp. 1–7, USENIX Association, 2010.

[19] A. De Luca, A. Hang, E. von Zezschwitz, and H. Hussmann, "I feel like i'm taking selfies all day!: Towards understanding biometric authentication on smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, (New York, NY, USA), pp. 1411–1414, ACM, 2015.

[20] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, "Casa: Context-aware scalable authentication," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, (New York, NY, USA), pp. 3:1–3:10, ACM, 2013.

[21] A. Gupta, M. Miettinen, N. Asokan, and M. Nagy, "Intuitive security policy configuration in mobile devices using context profiling," in *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, pp. 471–480, Sept 2012.

[22] N. Micallef, M. Just, L. Baillie, M. Halvey, and H. G. Kayacik, "Why aren't users using protection? investigating the usability of smartphone locking," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '15, (New York, NY, USA), pp. 284–294, ACM, 2015.

[23] M. Khamis, M. Hassib, E. v. Zezschwitz, A. Bulling, and F. Alt, "Gazetouchpin: Protecting sensitive data on mobile devices using secure multimodal authentication," in *Proceedings of the 19th ACM International Conference on Multimodal Interaction*, ICMI 2017, (New York, NY, USA), ACM, 2017.

[24] D. Buschek, F. Hartmann, E. von Zezschwitz, A. De Luca, and F. Alt, "Snapapp: Reducing authentication overhead with a time-constrained fast unlock option," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, (New York, NY, USA), ACM, 2016.

[25] burakgon, "App locker — best applock." Website, 2018. Retrieved June 4, 2018 from `https://play.google.com/store/apps/details?id=com.martianmode.applock`.

[26] D. Lab, "App lock." Website, 2018. Retrieved June 4, 2018 from `https://play.google.com/store/apps/details?id=com.domobile.applock`.